

MATH 101 - SETS, GROUPS, AND TOPOLOGY, FALL 2018
ASSIGNMENT 10

Due Friday, October 19 at the beginning of class (please submit your assignment on Canvas). Make sure to include your full name *and the list of your collaborators* (if any) with your assignment. You may discuss problems with others, but you may *not* keep a written record of your discussions. Please refer to the syllabus for details.

In your proofs, you may assume basic facts about real numbers and integers, such as those mentioned on p. 90-91 of Hammack. You also can use results from the course textbooks, results covered in class, or results you have proven already. As a general rule, you should imagine that you are writing your proof to convince somebody else in the class who is very skeptical about the particular statement. In particular, it should be completely understandable to another student: always justify your reasoning in plain English.

- (1) List all the subgroups of D_3 , the group of symmetries of an equilateral triangle.
- (2) Assume that G is a group. Recall (see p. 36 in Judson) that for $n \in \mathbb{N}$ and $a \in G$, a^n is defined to be the product (using the group operation) of a with itself n times. For example, $a^1 = a$, $a^2 = aa$, $a^3 = aaa$, etc.
 - (a) Assume that G is *abelian* and $a, b \in G$. Prove carefully that for any natural number n , $(ab)^n = a^n b^n$. *Hint: induction.*
 - (b) Give an example showing that the previous result is not true for all groups.
 - (c) Assume that G is abelian. Prove that $\{a \in G \mid a^2 = e\}$ is a subgroup of G .
- (3) Assume G is a group. Is the intersection of two subgroups of G a subgroup of G ? What about the union of two subgroups of G ?
- (4) Assume that $(G, *G)$ and $(H, *H)$ are groups. We define a binary operation $*$ on $G \times H$ (the cartesian product of G and H) as follows: $(g_1, h_1) * (g_2, h_2) = (g_1 *G g_2, h_1 *H h_2)$.
 - (a) Prove that $(G \times H, *)$ is a group (it is called the *direct product* of G and H , and is usually just written $G \times H$).
 - (b) If G has order n and H has order m (for $m, n \in \mathbb{N}$), what is the order of $G \times H$ (recall that the order of a group is the number of elements in the group)?
- (5) For this problem, fix a natural number n . It may be beneficial to read the first part of section 3.1 in Judson regarding the integers mod n . Recall: for a, b integers, we say that (by definition) a is *congruent to b modulo n* , written $a \equiv b \pmod{n}$ if n divides $a - b$. We will also write $a \equiv_n b$ to mean that a is congruent to b modulo n . Recall (Example 11.8 in Hammack) that \equiv_n is an equivalence relation on \mathbb{Z} . We define the set \mathbb{Z}_n to be the set of equivalence classes of the integers modulo n . That is, $\mathbb{Z}_n = \{[0], [1], [2], \dots, [n-1]\}$.

- (a) Assume that a, b, c, d are integers and n is a natural number. Assume that $a \equiv_n c$ and $b \equiv_n d$. Prove (using the definition of congruence modulo n) that $a + b \equiv_n c + d$.
- (b) We define a relation R from $\mathbb{Z}_n \times \mathbb{Z}_n$ to \mathbb{Z}_n by $(x, y)Rz$ if and only if there exists integers a, b, c so that $x = [a]$, $y = [b]$, $z = [c]$, and $a + b \equiv_n c$. Use the previous part to prove that R is a function from $\mathbb{Z}_n \times \mathbb{Z}_n$ to \mathbb{Z}_n . What is the output of $([a], [b])$ under this function?
- (c) The previous exercise showed that R defines a binary operation, which is just “addition modulo n ”. We will write $+$ for this operation. Show that $(\mathbb{Z}_n, +)$ is a group.
- (d) Convince yourself that one can similarly define a \cdot operation on \mathbb{Z}_n (multiplication modulo n) such that $[a] \cdot [b] = [a \cdot b]$ (you do not need to write anything). Answer the following:
- Is (\mathbb{Z}_n, \cdot) a group?
 - Prove the following general result: assume $*$ is a binary operation on a set G that satisfies the first two axioms of groups (associativity and existence of an identity e). Show that the set $H = \{a \in G \mid a \text{ has an inverse in } G\}$ is a group under the operation $*$. Deduce that the set of elements $[x]$ in \mathbb{Z}_n such that there is $[y] \in \mathbb{Z}_n$ with $[x] \cdot [y] = [1]$ is a group under multiplication modulo n . This group is called the group of *units* modulo n , and written $U(n)$.
 - List all the elements of $U(9)$.
- (6) (Extra credit) Assume G is a group such that for all $a \in G$, $a^2 = e$. Prove that G is abelian.